

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC996 U.S. PTC
09/924443
08/09/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日
Date of Application:

2001年 1月11日

出 願 番 号
Application Number:

特願2001-003467

出 願 人
Applicant(s):

沖電気工業株式会社



26694

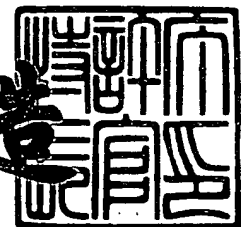
PATENT TRADEMARK OFFICE

ONISHI
31869-174125
8-9-01

2001年 5月18日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



CERTIFIED COPY OF
PRIORITY DOCUMENT

出証番号 出証特2001-3041269

【書類名】 特許願

【整理番号】 MA001307

【提出日】 平成13年 1月11日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00 630

【発明者】

 【住所又は居所】 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社
社内

 【氏名】 大西 一三

【特許出願人】

 【識別番号】 000000295

 【氏名又は名称】 沖電気工業株式会社

 【代表者】 篠塚 勝正

【代理人】

 【識別番号】 100083840

 【弁理士】

 【氏名又は名称】 前田 実

【手数料の表示】

 【予納台帳番号】 007205

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9003703

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 間欠信号の暗号化伝送システム

【特許請求の範囲】

【請求項 1】 第 1 通信装置から第 2 通信装置に間欠信号を伝送する際に、第 1 通信装置では、内部に備えられた暗号化回路で該間欠信号に対して暗号化を実施してから送信回路で送出し、第 2 通信装置では、内部に備えられた受信回路で受信した前記間欠信号を復号化回路で復号する暗号化伝送システムであって、

前記第 1 通信装置は、暗号化前の第 1 の間欠信号に基づいて第 2 の間欠信号用の送信側秘話鍵を生成する送信側秘話鍵生成回路と、該送信側秘話鍵を第 2 の間欠信号の暗号化に用いるために遅延させる送信側メモリとを有し、

前記第 2 通信装置は、復号化後の第 1 の間欠信号に基づいて第 2 の間欠信号用の受信側秘話鍵を生成する受信側秘話鍵生成回路と、該受信側秘話鍵を第 2 の間欠信号の暗号化に用いるために遅延させる受信側メモリとを有することを特徴とする暗号化伝送システム。

【請求項 2】 前記第 2 通信装置は、前記受信回路から出力される復号前の前記間欠信号中の伝送エラーを検出して、秘話初期化制御用の間欠信号を生成する初期化制御信号生成回路と、該秘話初期化制御用の間欠信号を第 1 通信装置に送出できる送信回路とを有し、

前記第 1 通信装置は、前記秘話初期化制御用の間欠信号を受信した場合、前記送信側秘話鍵生成回路、送信側メモリ、および、暗号化回路に対して初期化信号を送出する受信回路を有することを特徴とする請求項 1 に記載の暗号化伝送システム。

【請求項 3】 前記第 1 通信装置は、暗号化前の間欠信号に対してスクランブル処理を施すスクランブル回路と、該スクランブル回路に供給する擬似ランダムパターンを発生させる擬似ランダムパターン発生回路とを有し、

前記第 2 通信装置は、復号化後の間欠信号に対してデスクランブル処理を施すデスクランブル回路と、該デスクランブル回路に供給する擬似ランダムパターンを発生させる擬似ランダムパターン発生回路とを有することを特徴とする請求項 1 または 2 に記載の暗号化伝送システム。

【請求項 4】 前記第 1 通信装置および前記第 2 通信装置は、無線方式あるいは有線方式で双方向に間欠信号を送信でき、第 2 通信装置は、前記第 1 通信装置と同様に暗号化回路、送信回路、送信側秘話鍵生成回路、および、送信側メモリを備え、第 1 通信装置は、前記第 2 通信装置と同様に受信回路、復号化回路、受信側秘話鍵生成回路、および、受信側メモリを備えることを特徴とする請求項 1 ～ 3 の何れかに記載の暗号化伝送システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数の通信装置が各通信装置間において信号を送信する際に暗号化を実施する暗号化伝送システムに関し、特に、パケット通信方式のような間欠信号を各通信装置間において送信する際に暗号化を実施できる暗号化伝送システムに関する。

【0002】

【従来の技術】

従来の秘話通信を実施する暗号化伝送システムは、以下のように構成される。

【0003】

図 8 は、従来の暗号化伝送システムの概略構成を示す図である。

【0004】

第 1 通信装置 220 と第 2 通信装置 280 とは伝送路 300 により通信接続されている。伝送路 300 は、銅線あるいは光ファイバ等の有線接続と、電波あるいは赤外線等の無線接続の双方を含む伝送路である。

【0005】

第 1 通信装置 220 は、大きく分けて送信側回路と受信側回路とに分かれており、送信側回路には、送信信号 A を例えば符号の順序入れ替え等の手法によりスクランブル化してスクランブル信号 CA を出力するスクランブル回路 221 と、そのスクランブル回路 221 に擬似ランダムパターン RA1 を供給する擬似ランダムパターン発生回路 222 と、スクランブル信号 CA をさらに変調させた変調信号 MCA として送信する送信回路 223 とを有している。

【 0 0 0 6 】

一方、第 1 通信装置 2 2 0 の受信側回路には、受信した変調信号 M C B を復調させてスクランブル信号 C B を出力する受信回路 2 3 0 と、スクランブル信号 C B をデスクランブル化した受信信号 B として出力するデスクランブル回路 2 3 1 と、そのデスクランブル回路 2 3 1 に擬似ランダムパターン R A 2 を供給する擬似ランダムパターン発生回路 2 3 2 とを有している。

【 0 0 0 7 】

第 2 通信装置 2 8 0 も、第 1 の通信装置 2 2 0 と同様に、大きく分けて送信側回路と受信側回路とに分かれており、送信側回路には、送信信号 B をスクランブル化してスクランブル信号 C B を出力するスクランブル回路 2 8 1 と、そのスクランブル回路 2 8 1 に擬似ランダムパターン R A 2 を供給する擬似ランダムパターン発生回路 2 8 2 と、スクランブル信号 C B をさらに変調させた変調信号 M C B として送信する送信回路 2 8 3 とを有し、第 2 通信装置 2 8 0 の受信側回路には、受信した変調信号 M C A を復調させてスクランブル信号 C A を出力する受信回路 2 9 0 と、スクランブル信号 C A をデスクランブル化した受信信号 A として出力するデスクランブル回路 2 9 1 と、そのデスクランブル回路 2 9 1 に擬似ランダムパターン R A 1 を供給する擬似ランダムパターン発生回路 2 9 2 とを有している。

【 0 0 0 8 】

上記のように図 8 の第 1 通信装置 2 2 0 および第 2 通信装置 2 8 0 には、各々送信回路および受信回路を備えて双方向送受信が可能な構成を有しているが、一方向の送受信は逆方向の送受信と符号が異なるのみであるので、以下に記載する図 8 の暗号化伝送システムの動作の説明では、第 1 通信装置 2 2 0 から信号 A を第 2 通信装置 2 8 0 へ送信する場合のみを記載し、逆方向への信号 B の送信については記載を省略する。

【 0 0 0 9 】

第 1 通信装置 2 2 0 において、信号 A がスクランブル回路 2 2 1 に入力されると、スクランブル回路 2 2 1 では、擬似ランダムパターン発生回路 2 2 2 から入力される擬似ランダムパターン R A 1 により信号 A に対するスクランブル化が実施され、スクランブル信号 C A が出力される。

【 0 0 1 0 】

スクランブル信号C Aが送信回路2 2 3に入力されると、送信回路2 2 3では、スクランブル信号C Aに対して送信信号とするための変調が実施され、変調信号M C Aが伝送路3 0 0に出力される。

【 0 0 1 1 】

伝送路3 0 0から第2通信回路2 8 0に変調信号M C Aが入力されると、受信回路2 9 0では、変調信号M C Aが復調されてスクランブル信号C Aが出力される。

【 0 0 1 2 】

スクランブル信号C Aがデスクランブル回路2 9 1に入力されると、デスクランブル回路2 9 1では、擬似ランダムパターン発生回路2 9 2から入力される擬似ランダムパターンR A 1により信号Aに対するデスクランブル化が実施され、復号された信号Aが出力される。

【 0 0 1 3 】

ところが、図8に示した従来の暗号化伝送システムでは、ランダムパターンが固定であり、変換規則および変換周期等を同仕様で多数の通信装置を制作した場合には、第3者の解読可能性を0に近づけて秘話性を高めようとする、長い擬似ランダムパターンR A 1を用いることになる。すると、回路規模が増大してコストも増加するという問題がある。その問題を解決するために、例えば、特開平05-007202号公報に記載されたように、簡単な構成で秘話性も高い暗号化伝送システムが知られている。

【 0 0 1 4 】

図9は、特開平05-007202号公報に記載された従来の暗号化伝送システムの概略構成を示す図である。

【 0 0 1 5 】

図9の暗号化伝送システムでは、例えば、図8の暗号化伝送システムにおける擬似ランダムパターン発生回路2 2 2および2 9 2等無くし、代わりに受信信号を暗号化のための鍵情報として用いるように構成している。

【 0 0 1 6 】

第1通信装置200は、その送信側回路側に、受信した信号B' から得られた鍵信号を用いて送信する信号Aを暗号化して暗号化信号CAを出力する変換部201と、暗号化信号CAをさらに変調させた変調信号MCAとして送信する送信回路203とを有している。また、受信側回路側には、受信した変調信号MCBを復調させて暗号化信号CBを出力する受信回路210と、暗号化信号CBを逆変換した信号B' として出力する逆変換部211と、その逆変換部211に逆変換用の鍵情報として格納しておいた信号Aを供給するメモリ202とを有している。メモリ202には、送信する信号Aが変換部201に入力される時に、信号Aが並列に入力されて格納される。

【0017】

第2通信装置260は、第1通信装置200と同様に、送信側回路側に、受信した信号A' から得られた鍵信号を用いて送信する信号Bを暗号化して暗号化信号CBを出力する変換部261と、暗号化信号CBをさらに変調させた変調信号MCBとして送信する送信回路263とを有しており、受信側回路側には、受信した変調信号MCAを復調させて暗号化信号CAを出力する受信回路270と、暗号化信号CAを逆変換した信号A' として出力する逆変換部271と、その逆変換部271に逆変換用の鍵情報として格納しておいた信号Bを供給するメモリ262とを有している。メモリ262には、送信する信号Bが変換部261に入力される時に、信号Bが並列に入力されて格納される。

【0018】

図9の暗号化伝送システムでは、上記のように、送信信号Aについては受信信号B' を鍵情報として利用し、且つ、受信した暗号化信号CBを逆変換するためには、送信した信号Aを利用しているので、簡単な構成で高い秘話性を得ることができる。

【0019】

【発明が解決しようとする課題】

しかしながら、上記した図9の従来の暗号化伝送システムでは、受信した暗号化信号CBを逆変換するために送信した信号Aを利用しているので、送信信号と受信信号の連続性が途切れると、逆変換するための鍵情報が変換時の鍵情報と一

致しなくなるので、暗号化伝送ができなくなるという問題があった。

【 0 0 2 0 】

すなわち、信号 A を第 1 通信装置 2 0 0 から送信した場合、第 2 通信装置 2 6 0 では信号 B を送信するために受信した信号 A' を鍵情報として用いて変換した暗号化信号 C B としてから送信し、第 1 通信装置 2 0 0 では受信した暗号化信号 C B をメモリに格納しておいた信号 A を鍵情報として逆変換するが、信号 A が、例えば、A 1、A 2、A 3、・・・のように連続して間断なく出力されないと、第 1 通信装置 2 0 0 のメモリ 2 0 2 に格納しておいた信号 A と、第 2 通信装置 2 6 0 で鍵情報として利用した信号 A' が一致しなくなり、その結果、暗号化した信号を元に戻せなくなり、秘話通信ができなくなるという問題があった。

【 0 0 2 1 】

上記のように、図 9 の暗号化伝送システムは、信号 A が間断なく出力されないと秘話通信できなくなるので、例えば、I P（インターネット・プロトコル）パケット伝送のような間欠的にデータが流れる伝送経路では用いることができなかった。

【 0 0 2 2 】

本発明は、上述した如き従来の問題を解決するためになされたものであって、I P パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施できる簡単な構成の暗号化伝送システムを提供することを目的とする。

【 0 0 2 3 】

【課題を解決するための手段】

上述の目的を達成するため、請求項 1 に記載した本発明の暗号化伝送システムは、第 1 通信装置から第 2 通信装置に間欠信号を伝送する際に、第 1 通信装置では、内部に備えられた暗号化回路で該間欠信号に対して暗号化を実施してから送信回路で送出し、第 2 通信装置では、内部に備えられた受信回路で受信した間欠信号を復号化回路で復号する暗号化伝送システムであって、第 1 通信装置は、暗号化前の第 1 の間欠信号に基づいて第 2 の間欠信号用の送信側秘話鍵を生成する送信側秘話鍵生成回路と、該送信側秘話鍵を第 2 の間欠信号の暗号化に用いるために遅延させる送信側メモリとを有し、第 2 通信装置は、復号化後の第 1 の間欠

信号に基づいて第 2 の間欠信号用の受信側秘話鍵を生成する受信側秘話鍵生成回路と、該受信側秘話鍵を第 2 の間欠信号の暗号化に用いるために遅延させる受信側メモリとを有することを特徴とする。

【 0 0 2 4 】

また、請求項 2 の本発明は、請求項 1 に記載の暗号化伝送システムにおいて、第 2 通信装置は、受信回路から出力される復号前の間欠信号中の伝送エラーを検出して、秘話初期化制御用の間欠信号を生成する初期化制御信号生成回路と、該秘話初期化制御用の間欠信号を第 1 通信装置に送出できる送信回路とを有し、第 1 通信装置は、秘話初期化制御用の間欠信号を受信した場合、送信側秘話鍵生成回路、送信側メモリ、および、暗号化回路に対して初期化信号を送出する受信回路を有することを特徴とする。

【 0 0 2 5 】

また、請求項 3 の本発明は、請求項 1 または 2 に記載の暗号化伝送システムにおいて、第 1 通信装置は、暗号化前の間欠信号に対してスクランブル処理を施すスクランブル回路と、該スクランブル回路に供給する擬似ランダムパターンを発生させる擬似ランダムパターン発生回路とを有し、第 2 通信装置は、復号化後の間欠信号に対してデスクランブル処理を施すデスクランブル回路と、該デスクランブル回路に供給する擬似ランダムパターンを発生させる擬似ランダムパターン発生回路とを有することを特徴とする。

【 0 0 2 6 】

また、請求項 4 の本発明は、請求項 1 ～ 3 の何れかに記載の暗号化伝送システムにおいて、第 1 通信装置および第 2 通信装置は、無線方式あるいは有線方式で双方向に間欠信号を伝送でき、第 2 通信装置は、第 1 通信装置と同様に暗号化回路、送信回路、送信側秘話鍵生成回路、および、送信側メモリを備え、第 1 通信装置は、第 2 通信装置と同様に受信回路、復号化回路、受信側秘話鍵生成回路、および、受信側メモリを備えることを特徴とする。

【 0 0 2 7 】

【発明の実施の形態】

以下、本発明を図示した実施形態に基づいて説明する。

【 0 0 2 8 】

図 1 は、本発明の第 1 の実施形態の暗号化伝送システムの構成を示すブロック図である。また、図 1 中で図 8 及び図 9 に示した従来の暗号化システムと同じ機能の部分については、図 8 または図 9 と同じ符号を用いて重複する記載を省略する。

【 0 0 2 9 】

第 1 通信装置 1 は、暗号化送信部 1 0 と受信復号部 2 0 とに分かれており、暗号化送信部 1 0 には、間欠信号の一種であるパケット信号で構成される送信信号 A を例えば符号の順序入れ替え等の手法により暗号化して暗号化信号 C A を出力する暗号化回路 1 1 と、パケット信号の暗号化信号 C A をさらに変調させた変調信号 M C A として送信する送信回路 1 2 と、暗号化回路 1 1 に供給するための秘話鍵 K A をパケット信号の送信信号 A から生成する秘話鍵生成回路 1 3 と、前回のパケット信号である送信信号 A により秘話鍵生成回路 1 3 で生成された秘話鍵 K A を次回のパケット信号を暗号化させるために格納して遅延させるメモリ 1 4 とを有している。

【 0 0 3 0 】

一方、第 1 通信装置 1 の受信復号部 2 0 には、受信した変調信号 M C B を復調させて暗号化信号 C B を出力する受信回路 2 1 と、暗号化信号 C B を復号化した受信信号 B' として出力する復号化回路 2 2 と、その復号化回路 2 2 に供給するための秘話鍵 K B をパケット信号である受信信号 B' から生成する秘話鍵生成回路 2 3 と、前回のパケット信号である受信信号 B' により秘話鍵生成回路 2 3 で生成された秘話鍵 K B を次回のパケット信号を暗号化させるために格納して遅延させるメモリ 2 4 とを有している。

【 0 0 3 1 】

第 2 通信装置 6 も、第 1 の通信装置 1 と同様に、大きく分けて暗号化送信部 7 0 と受信復号部 6 0 とに分かれており、暗号化送信部 7 0 には、送信信号 B を暗号化して暗号化信号 C B を出力する暗号化回路 7 1 と、パケット信号である暗号化信号 C B をさらに変調させた変調信号 M C B として送信する送信回路 7 2 と、暗号化回路 7 1 に供給するための秘話鍵 K B をパケット信号である送信信号 B か

ら生成する秘話鍵生成回路 7 3 と、前回のパケット信号である送信信号 B により秘話鍵生成回路 7 3 で生成された秘話鍵 K B を次の回のパケット信号を暗号化させるために格納して遅延させるメモリ 7 4 とを有し、第 2 通信装置 6 の受信復号部 6 0 には、受信した変調信号 M C A を復調させて暗号化信号 C A を出力する受信回路 6 1 と、暗号化信号 C A を復号化した受信信号 A' として出力する復号化回路 6 2 と、その復号化回路 6 2 に供給するための秘話鍵 K A をパケット信号である受信信号 A' から生成する秘話鍵生成回路 6 3 と、前回のパケット信号である受信信号 A' により秘話鍵生成回路 6 3 で生成された秘話鍵 K A を次のパケット信号を暗号化させるために格納して遅延させるメモリ 6 4 とを有している。

【 0 0 3 2 】

上記のように図 1 の第 1 通信装置 1 および第 2 通信装置 6 には、各々暗号化送信部 1 0、7 0 回路および受信復号部 2 0、6 0 を備えて双方向送受信が可能な構成を有しているが、例えば、暗号化送信部 1 0 から受信復号部 6 0 への方向の送受信は、暗号化送信部 7 0 から受信復号部 2 0 への逆方向の送受信と符号が異なるのみである。そこで、以下に記載する図 1 の暗号化伝送システムの動作の説明では、図 1 から一方向の送受信に関するブロックのみを抜き出した図 2 に示したように、第 1 通信装置 1 から信号 A を第 2 通信装置 6 へ送信する場合のみを記載し、逆方向への信号 B の送信については記載を省略する。

【 0 0 3 3 】

図 3 (a) は、図 1 の第 1 通信装置 1 に入力されるパケット信号の送信信号 A を時系列に示した図であり、図 3 (b) は、図 1 の第 1 通信装置 1 中の暗号化回路 1 1 から出力されるパケット信号の暗号化信号 C A を時系列に示した図であり、図 3 (c) は、図 1 の第 2 通信装置 6 から出力されるパケット信号の受信信号 A' を時系列に示した図である。

【 0 0 3 4 】

第 1 通信装置 1 において、最初にパケット信号の信号 A が暗号化回路 1 1 に入力されると、暗号化回路 1 1 では、メモリ 1 4 から入力される遅延された秘話鍵 D K A により信号 A に対する暗号化が実施され、暗号化信号 C A が出力される。

【 0 0 3 5 】

{信号 $A(n-2)$ の入力時: (n は 3 以上の正の整数) }

例えば、図 3 (a) に示したように、最初に信号 $A(n-2)$ が暗号化回路 11 に入力された場合について説明する。信号 $A(n-2)$ は、暗号化回路 11 で、メモリ 14 に格納されていた初期値 (例えばオール 0 等) により暗号化されて、図 3 (b) に示したように暗号化信号 $CA(n-2)$ が出力される。また、上記の処理と平行して信号 $A(n-2)$ は秘話鍵生成回路 13 にも入力され、秘話鍵生成回路 13 では秘話鍵 $KA(n-2)$ が生成されてメモリ 14 に格納される。暗号化信号 $CA(n-2)$ は送信回路 12 で変調信号 $MCA(n-2)$ に変調されて第 2 通信装置 6 に送出される。

【 0 0 3 6 】

第 2 通信装置 6 の受信回路 61 は、変調信号 $MCA(n-2)$ を受信すると復調を実施して暗号化信号 $CA(n-2)$ を復号化回路 62 に出力する。復号化回路 62 では、暗号化信号 $CA(n-2)$ に対して、メモリ 64 に格納されていた初期値 (例えばオール 0 等) を用いて復号化を実施し、図 3 (c) に示したように信号 $A'(n-2)$ を出力する。信号 $A'(n-2)$ は第 2 通信装置 6 から外部に出力されると同時に秘話鍵生成回路 63 にも入力される。秘話鍵生成回路 63 では信号 $A'(n-2)$ に基づいて秘話鍵 $KA(n-2)$ が生成されてメモリ 64 に格納される。

【 0 0 3 7 】

{信号 $A(n-1)$ の入力時: }

図 3 (a) に示したように、信号 $A(n-2)$ の次に信号 $A(n-1)$ が暗号化回路 11 に入力された場合について説明する。信号 $A(n-1)$ は、暗号化回路 11 で、メモリ 14 に格納されていた秘話鍵 $DKA(n-2)$ により暗号化されて、図 3 (b) に示したように暗号化信号 $CA(n-1)$ が出力される。また、上記の処理と平行して信号 $A(n-1)$ は秘話鍵生成回路 13 にも入力され、秘話鍵生成回路 13 では秘話鍵 $KA(n-1)$ が生成されてメモリ 14 に格納される。暗号化信号 $CA(n-1)$ は送信回路 12 で変調信号 $MCA(n-1)$ に変調されて第 2 通信装置 6 に送出される。

【 0 0 3 8 】

第2通信装置6の受信回路61は、変調信号MCA(n-1)を受信すると復調を実施して暗号化信号CA(n-1)を復号化回路62に出力する。復号化回路62では、暗号化信号CA(n-1)に対して、メモリ64に格納されていた秘話鍵DKA(n-2)を用いて復号化を実施し、図3(c)に示したように信号A'(n-1)を出力する。信号A'(n-1)は第2通信装置6から外部に出力されると同時に秘話鍵生成回路63にも入力される。秘話鍵生成回路63では信号A'(n-1)に基づいて秘話鍵KA(n-1)が生成されてメモリ64に格納される。

【0039】

{信号A(n)の入力時:}

図3(a)に示したように、信号A(n-2)、信号A(n-1)に続いて信号A(n)が暗号化回路11に入力された場合について説明する。信号A(n)は、暗号化回路11で、メモリ14に格納されていた秘話鍵DKA(n-1)により暗号化されて、図3(b)に示したように暗号化信号CA(n)が出力される。また、上記の処理と平行して信号A(n)は秘話鍵生成回路13にも入力され、秘話鍵生成回路13では秘話鍵KA(n)が生成されてメモリ14に格納される。暗号化信号CA(n)は送信回路12で変調信号MCA(n)に変調されて第2通信装置6に送出される。

【0040】

第2通信装置6の受信回路61は、変調信号MCA(n)を受信すると復調を実施して暗号化信号CA(n)を復号化回路62に出力する。復号化回路62では、暗号化信号CA(n)に対して、メモリ64に格納されていた秘話鍵DKA(n-1)を用いて復号化を実施し、図3(c)に示したように信号A'(n)を出力する。信号A'(n)は第2通信装置6から外部に出力されると同時に秘話鍵生成回路63にも入力される。秘話鍵生成回路63では信号A'(n)に基づいて秘話鍵KA(n)が生成されてメモリ64に格納される。

【0041】

{信号A(n+1)の入力時:}

上記と同様にして、第1通信装置1の暗号化回路11に信号A(n+1)が入

力されると、秘話鍵DKA (n) による暗号化が実施されて暗号化信号CA (n + 1) が送出される。また第2通信装置6の復号化回路62に暗号化信号CA (n + 1) が入力されると、秘話鍵DKA (n) による復号化が実施されて信号A' (n + 1) が出力される。

【0042】

このように、本実施形態では、送信側で1つ前のパケット信号から生成された秘話鍵を用いて次のパケット信号の暗号化を実施し、受信側でも1つ前のパケット信号から生成された秘話鍵を用いて次のパケット信号の復号化を実施するように構成したので、簡単な構成でも秘話鍵が順次変化することから第3者が解読することが困難であり、パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施することができる。

【0043】

ところで、上記した第1の実施形態では、第1通信装置1から送信したパケット信号が伝送経路の異常等により第2通信装置6に正常に届かない場合には、次のパケット信号の秘話鍵が送信側と受信側で一致しなくなるので、以後の暗号化通信ができなくなるという問題があった。そこで、次の第2の実施形態では、伝送経路等に異常が発生した場合に、第1通信装置1および第2通信装置6を初期化して再度暗号化通信を再開できる暗号化伝送システムについて説明する。

【0044】

図4は、本発明の第2の実施形態の暗号化伝送システムの構成を示すブロック図である。

【0045】

図4に示した第2の実施形態と図1に示した第1の実施形態との違いは、主に第1通信装置2および第2通信装置7内に、相対する各通信装置の暗号化回路等を初期化するための初期化制御信号IPA、IPBを生成するための回路（初期化生成回路35、95）を有している点、その初期化制御信号IPA、IPBを相対する通信装置内の暗号化送信部30、90に向けて送出することにより、暗号化回路31、91、秘話鍵生成回路33、93、メモリ34、94、を初期化できる点である。

【 0 0 4 6 】

図 4 の第 1 通信装置 2 および第 2 通信装置 7 には、上記のように、各々暗号化送信部 3 0、9 0 回路および受信復号部 4 0、8 0 を備えて双方向送受信が可能な構成を有しているが、例えば、暗号化送信部 3 0 から受信復号部 8 0 の方向への送受信は、暗号化送信部 9 0 から受信復号部 4 0 への逆方向の送受信と符号が異なるのみである。そこで、以下に記載する図 4 の暗号化伝送システムの動作の説明では、図 4 から一方向の送受信に関するブロックのみを抜き出した図 5 に示したように、第 1 通信装置 2 から信号 A を第 2 通信装置 7 へ送信する場合のみを記載し、逆方向への信号 B の送信については記載を省略する。

【 0 0 4 7 】

図 6 (a) は、図 5 の第 1 通信装置 2 に入力されるパケット信号の送信信号 A が暗号化されて送信され、正常に第 2 通信装置 7 に受信されて復号化される場合のフローチャートであり、図 6 (b) は、図 5 の第 1 通信装置 2 から暗号化されて送信されたパケット信号の送信信号 A に伝送エラー（異常）が発生し、第 2 通信装置 7 で正常に受信できなかった場合のフローチャートである。

【 0 0 4 8 】

図 6 (a) の場合、すなわち、第 1 通信装置 2 から第 2 通信装置 7 に暗号化された信号が正常に（伝送エラーが無く）届いて、正常な復号が可能な場合には、上記した第 1 の実施形態と同様に、第 1 通信装置側で、前回のパケット信号から生成された秘話鍵により送信信号に暗号化処理が実施されて送出される（ステップ S 1）。また、第 2 通信装置側では、前回のパケット信号から生成された秘話鍵により受信信号に復号化処理（ステップ S 2）が実施される。

【 0 0 4 9 】

図 6 (b) の場合、すなわち、伝送エラーが発生する場合には、まず、第 1 通信装置側で、前回のパケット信号から生成された秘話鍵により送信信号に暗号化処理が実施されて送出されると（ステップ S 1 1）、第 2 通信装置側では、受信回路 8 1 で、受信したパケット信号の変調信号 M C A からフレーム・チェック・シーケンス（F C S）を検出することにより伝送エラーが発生したことを検知する（ステップ S 1 2）。F C S エラーを検出した受信回路 8 1 は、伝送エラーが

発生したことを示すエラー信号 E D A を初期化制御信号生成回路 9 5 に送信する。エラー信号 E D A を受信した初期化制御信号生成回路 9 5 では、第 1 通信装置 2 内の暗号化送信部 3 0 を初期化する保守用の初期化制御信号 I P A (パケット信号) を生成し、その初期化制御信号 I P A を送信回路 9 2 により第 1 通信装置 2 へ向けて送出する (ステップ S 1 3)。

【 0 0 5 0 】

初期化制御信号 I P A を受信した第 1 通信装置 2 内の受信回路 4 1 では、その初期化制御信号 I P A の受信をトリガとして、暗号化送信部 3 0 を初期化するための初期化指示信号 I C A を暗号化回路 3 1、秘話鍵生成回路 3 3、および、メモリ 3 4 に向けて送出する。受信回路 4 1 は、ステップ S 1 4 の処理を実施するとともに、初期化制御信号 I P A を正常に受信したことを示す I P A 正常受信信号 R I A を初期化制御信号生成回路 3 5 に出力する。I P A 正常受信信号 R I A を受信した初期化制御信号生成回路 3 5 では、第 2 通信装置 2 内の受信復号部 8 0 を初期化する保守用の初期化応答信号 I R A (パケット信号) を生成し、その初期化応答信号 I R A を送信回路 3 2 により第 2 通信装置 7 へ向けて送出する (ステップ S 1 4)。

【 0 0 5 1 】

初期化応答信号 I R A を受信した第 2 通信装置 7 内の受信回路 8 1 では、その初期化応答信号 I R A の受信をトリガとして、受信復号部 8 0 を初期化するための初期化指示信号 R C A を復号化回路 8 2、秘話鍵生成回路 8 3、および、メモリ 8 4 に向けて送出する (ステップ S 1 5)。

【 0 0 5 2 】

初期化された第 1 通信装置 2 内の暗号化送信部 3 0 では、メモリ 3 4 が初期値 (例えば、オール 0 等) となる。従って、暗号化回路 3 1 では、秘話鍵の初期値から暗号化を開始する (ステップ S 1 6)。この初期値により暗号化された変調信号 M C A が第 1 通信装置 2 から第 2 通信装置 7 に送出される。

【 0 0 5 3 】

第 2 通信装置 7 内の受信復号部 8 0 では、初期値により暗号化された変調信号 M C A が受信回路 8 1 で受信されると、秘話鍵の初期値から復号化を開始する (

ステップ S 1 7)。以後は、上記した第 1 の実施形態と同様に、第 1 通信装置 2 側で、前回のパケット信号から生成された秘話鍵により送信信号に暗号化処理が実施されて送出され（ステップ S 1 8）、第 2 通信装置側では、前回のパケット信号から生成された秘話鍵により受信信号に復号化処理（ステップ S 1 9）が実施される。

【 0 0 5 4 】

このように、本実施形態では、伝送エラー等により第 1 通信装置から送出されたパケット信号が正常に第 2 通信装置で受信されなかった場合には、初期化制御信号および初期化応答信号により第 1 通信装置の暗号化送信部と第 2 通信装置の受信復号部を初期化できるように構成したので、第 1 の実施形態と同様に、簡単な構成でも秘話鍵が順次変化することから第 3 者が解読することが困難であり、パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施することができることに加えて、間欠的にデータが流れる伝送経路で伝送エラーが発生する場合でも、暗号化した通信を実施することができる。

【 0 0 5 5 】

ところで、上記した第 1 の実施形態では、通信開始時には秘話鍵の初期値としてオール 0 等の固定値を用いることから、最初から傍受する第 3 者に対して暗号解読のための手がかりを与えてしまう可能性があり、第 2 の実施形態では、通信開始時に加えて、通信中の伝送エラーによる初期化時にも傍受する第 3 者に対して暗号解読のための手がかりを与えてしまう可能性がある。そこで、次の第 3 の実施形態では、通信開始時および通信中の初期化時にも、第 3 者に対して暗号解読のための手がかりを与えにくい暗号化伝送システムについて説明する。

【 0 0 5 6 】

図 7 は、本発明の第 3 の実施形態の暗号化伝送システムの構成を示すブロック図である。

【 0 0 5 7 】

図 7 に示した第 3 の実施形態と図 1 に示した第 1 の実施形態との違いは、主に第 1 通信装置 3 内に送信する信号 A を事前にスクランブル処理してスクランブル信号 S A を出力するスクランブル回路 5 6 と、そのスクランブル回路 5 6 に擬似

ランダムパターン R A を供給する擬似ランダムパターン発生回路 5 5 とを有し、第 2 通信装置 8 内に、復号化したスクランブル信号 S A をデスクランブル処理するデスクランブル回路 1 0 6 と、そのデスクランブル回路 1 0 6 に擬似ランダムパターン R A を供給する擬似ランダムパターン発生回路 1 0 5 とを有している点である。

【 0 0 5 8 】

そのため、第 1 通信装置 3 の暗号化回路 5 1 では、スクランブル信号 S A に対してさらに暗号化処理を実施した暗号化信号 C S A を出力するようになり、送信回路 5 2 では、暗号化信号 C S A に対して変調を実施した変調信号 M C S A を出力する。また、秘話鍵生成回路 5 3 は、スクランブル信号 S A に基づいて秘話鍵 K S A を生成し、メモリ 5 4 は、秘話鍵 K S A を格納することにより次のパケット信号が入力するまで遅延させた秘話鍵 D K S A を出力する。

【 0 0 5 9 】

また、第 2 通信装置 8 の受信回路 1 0 1 は、受信した変調信号 M C S A を復調して暗号化信号 C S A を出力し、復号化回路 1 0 2 は、暗号化信号 C S A を受信すると、その信号を復号してスクランブル信号 S A を出力する。また、スクランブル信号 S A は秘話鍵生成回路 1 0 3 にも入力される。秘話鍵生成回路 1 0 3 では、入力したスクランブル信号 S A に基づいて秘話鍵 K S A を生成し、メモリ 1 0 4 は、秘話鍵 K S A を格納することにより次の暗号化信号 C S A が入力するまで遅延させた秘話鍵 D K S A を出力する。

【 0 0 6 0 】

なお、図 7 に示した第 3 の実施形態は、図 1 に示した第 1 の実施形態にスクランブル回路等を付加したものであるが、同様にして図 4 に示した第 2 の実施形態に対してもスクランブル回路等を付加することができる。

【 0 0 6 1 】

このように、本実施形態では、通信開始時や通信中の伝送エラーによる初期化時に、最初からスクランブル処理された信号を用いるようにしたので、第 1 の実施形態と同様に、簡単な構成でも秘話鍵が順次変化することから第 3 者が解読することが困難であり、パケット伝送のような間欠的にデータが流れる伝送経路で

も暗号化した通信を実施することができること、および、第 2 の実施形態と同様に、間欠的にデータが流れる伝送経路で伝送エラーが発生する場合でも、暗号化した通信を実施することができることに加えて、最初から傍受する第 3 者に対して暗号解読のための手がかりを与えてしまう可能性を減らすことができる。

【0062】

なお、上記した各実施形態では、第 1 通信装置と第 2 通信装置との間の伝送として説明したが、本発明はこれに限られるものではなく、例えば、2 個以上の複数の通信装置を接続するネットワーク中から任意の 2 つの通信装置間でパケット信号のような間欠信号の送受信が実施される場合にも適用することができる。

【0063】

【発明の効果】

上記のように本発明では、通信開始時や通信中の伝送エラーによる初期化時に、最初からスクランブル処理された信号を用いるようにし、簡単な構成でも秘話鍵が順次変化するので、第 3 者が解読することが困難であることに加えて、パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施することができる。

【0064】

また、本発明では、上記した効果に加えて、間欠的にデータが流れる伝送経路で伝送エラーが発生する場合であっても、暗号化した通信を実施することができる。

【0065】

また、本発明では、上記した効果に加えて、最初から傍受する第 3 者に対して暗号解読のための手がかりを与えてしまう可能性を減らすことができる。

【図面の簡単な説明】

【図 1】 本発明の第 1 の実施形態の暗号化伝送システムの構成を示すブロック図である。

【図 2】 図 1 から一方向の送受信に関するブロックのみを抜き出した図である。

【図 3】 (a) は図 1 の第 1 通信装置に入力されるパケット信号の送信信

号を時系列に示した図であり、(b)は図1の第1通信装置中の暗号化回路から出力されるパケット信号の暗号化信号CAを時系列に示した図であり、(c)は図1の第2通信装置から出力されるパケット信号の受信信号A'を時系列に示した図である。

【図4】 本発明の第2の実施形態の暗号化伝送システムの構成を示すブロック図である。

【図5】 図4から一方向の送受信に関するブロックのみを抜き出した図である。

【図6】 (a)は図5の第1通信装置2から送信されたパケット信号が正常に第2通信装置7に受信される場合のフローチャートであり、(b)は図5の第1通信装置2から送信されたパケット信号に伝送エラーが生じて異常状態で第2通信装置7に受信される場合のフローチャートである。

【図7】 本発明の第3の実施形態の暗号化伝送システムの構成を示すブロック図である。

【図8】 従来の暗号化伝送システムの概略構成を示す図である。

【図9】 従来の暗号化伝送システムの概略構成を示す図である。

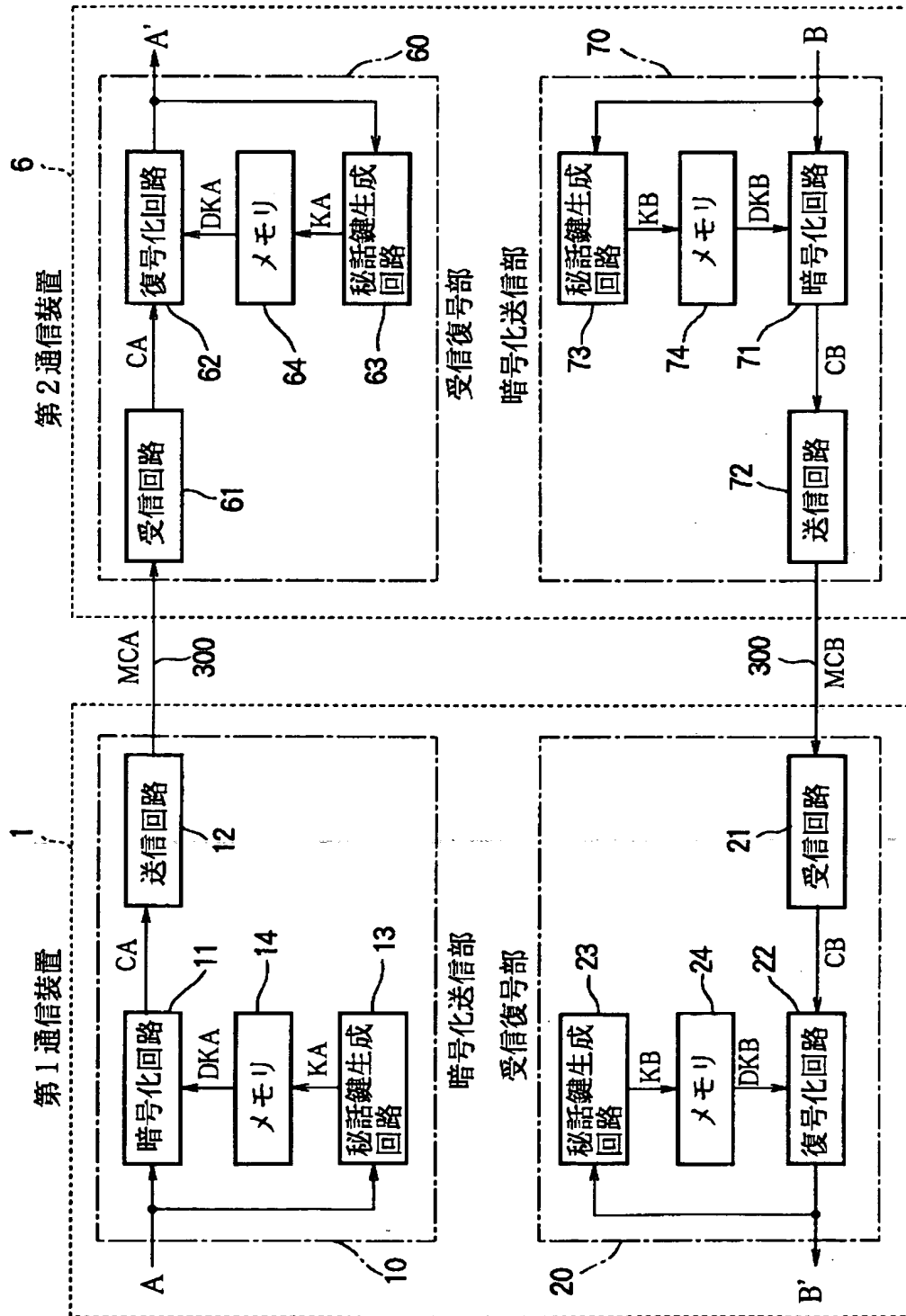
【符号の説明】

1 第1通信装置、 6 第2通信装置、 10、70 暗号化送信部、 20、60 受信復号部、 11、71 暗号化回路、 12、72 送信回路、 13、23、63、73 秘話鍵生成回路、 14、24、64、74 メモリ、 21、61 受信回路、 22、62 復号化回路、 300 伝送路。

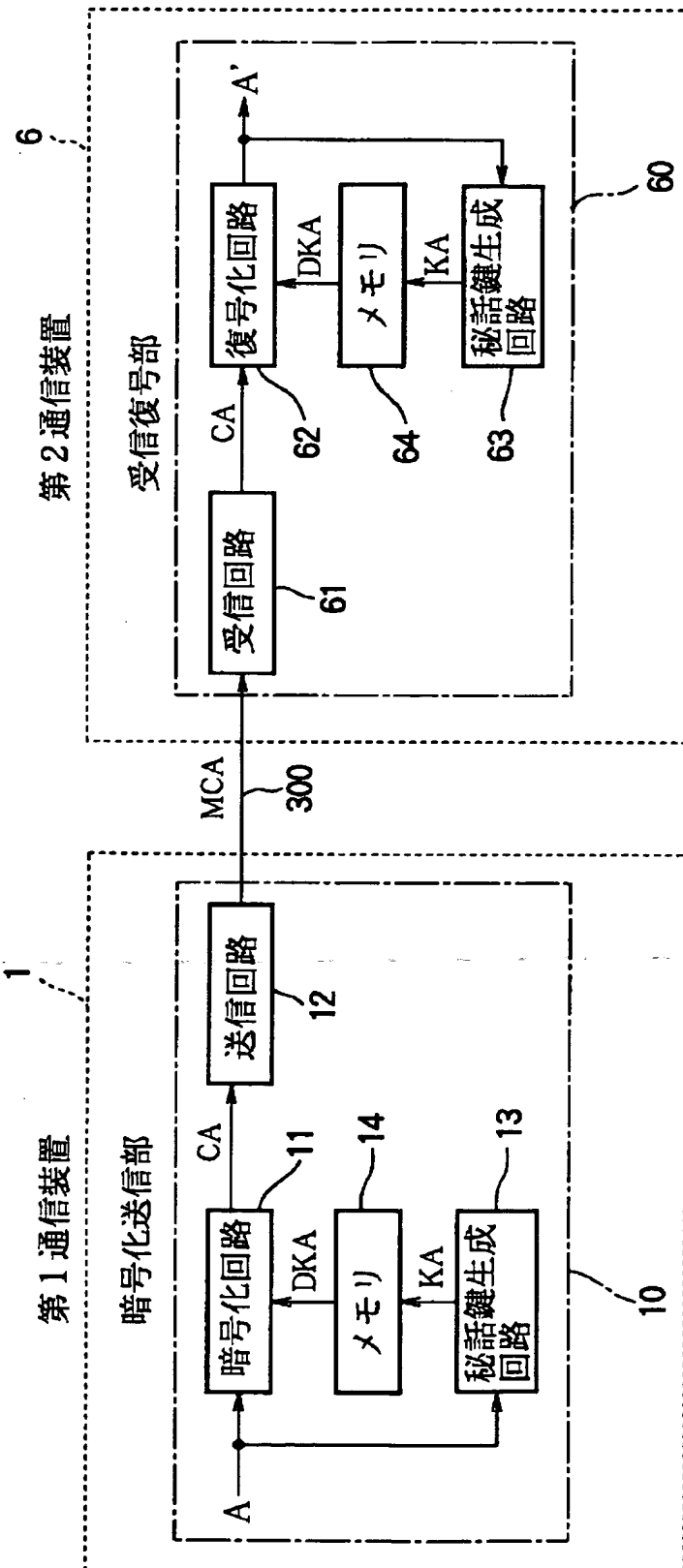
【書類名】

図面

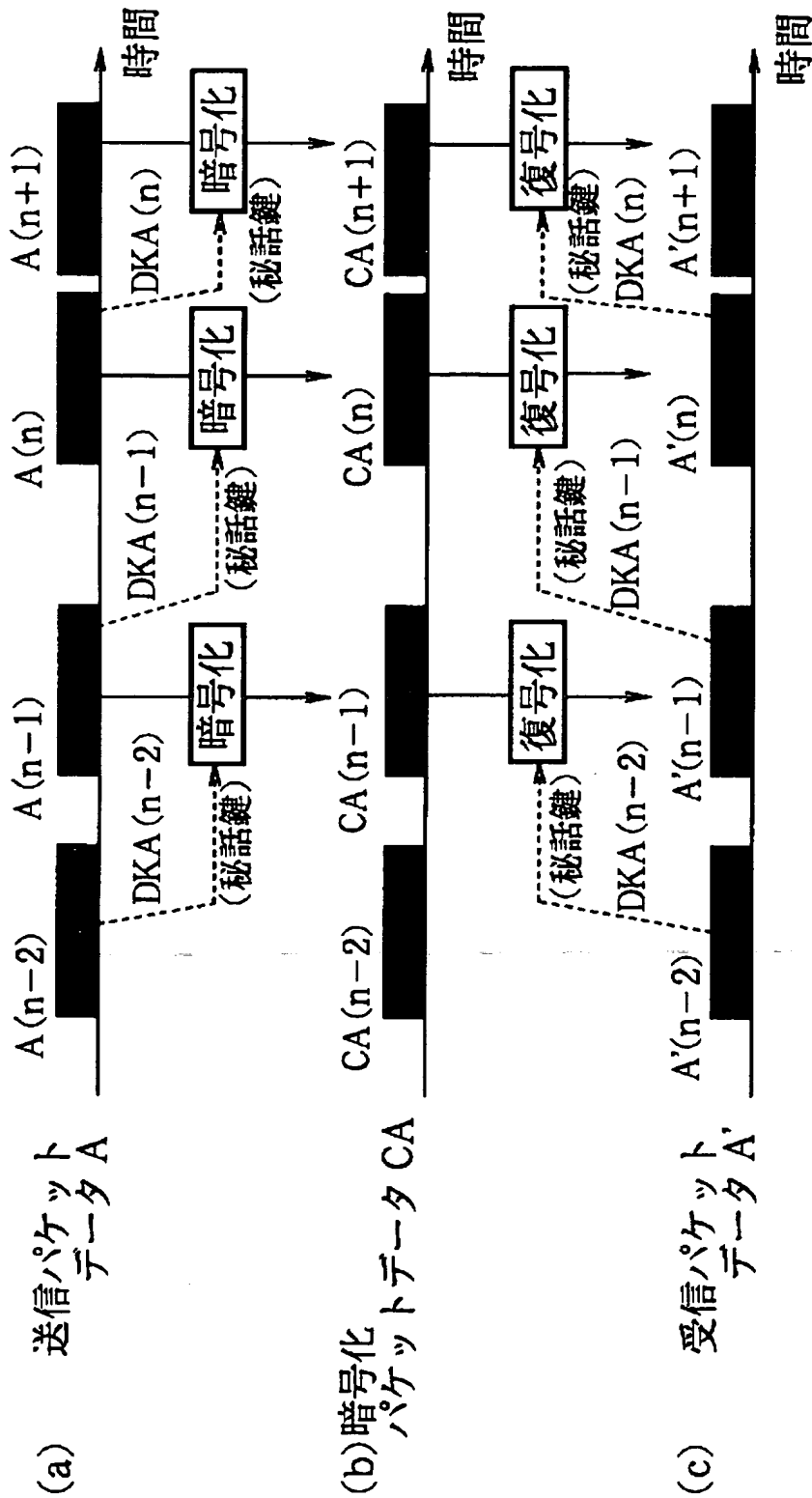
【図 1】



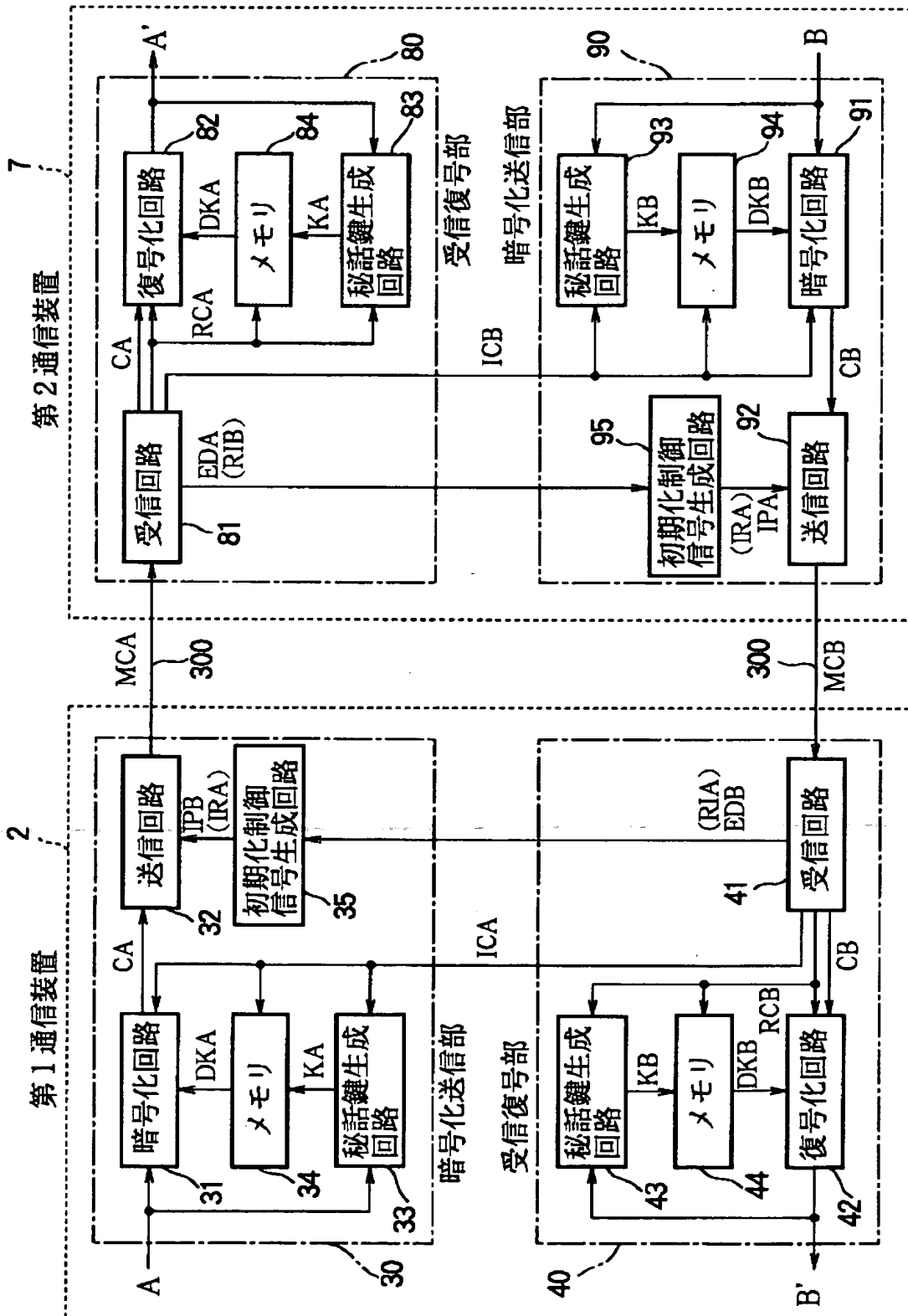
【図2】



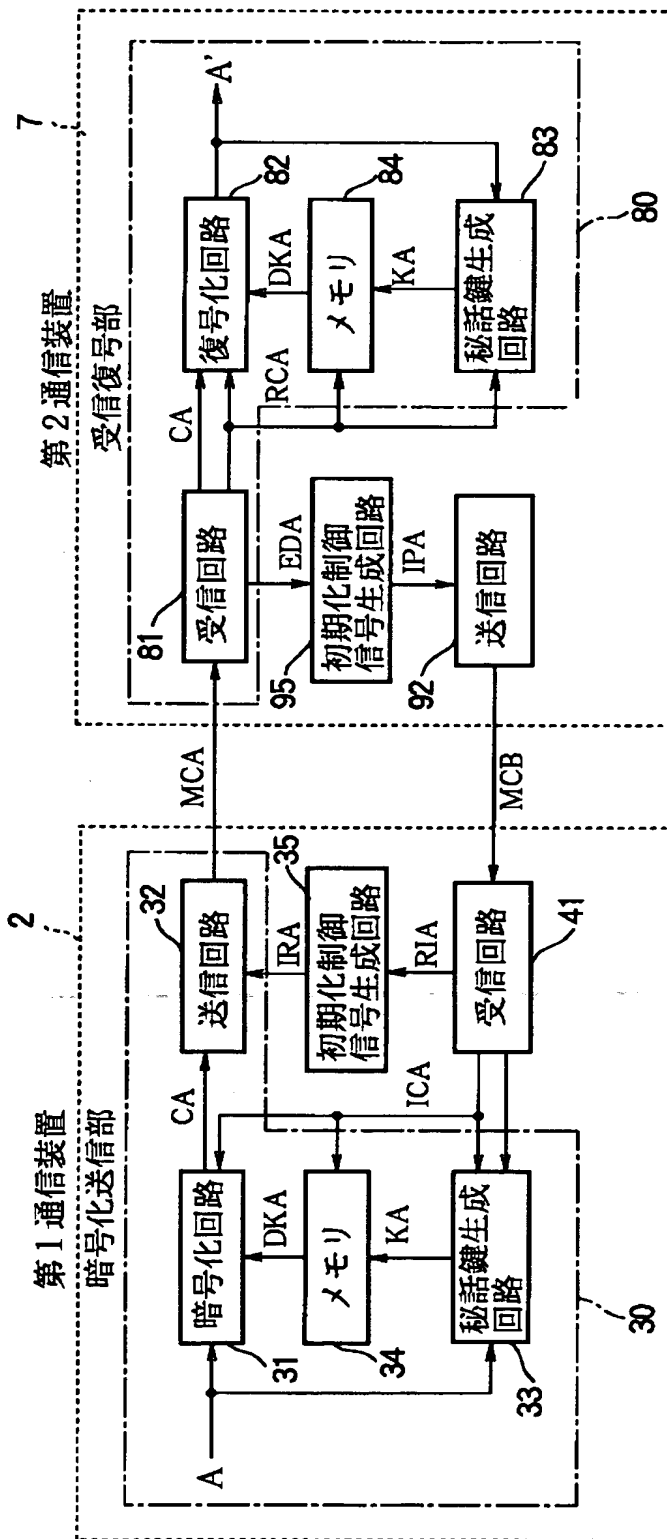
【図3】



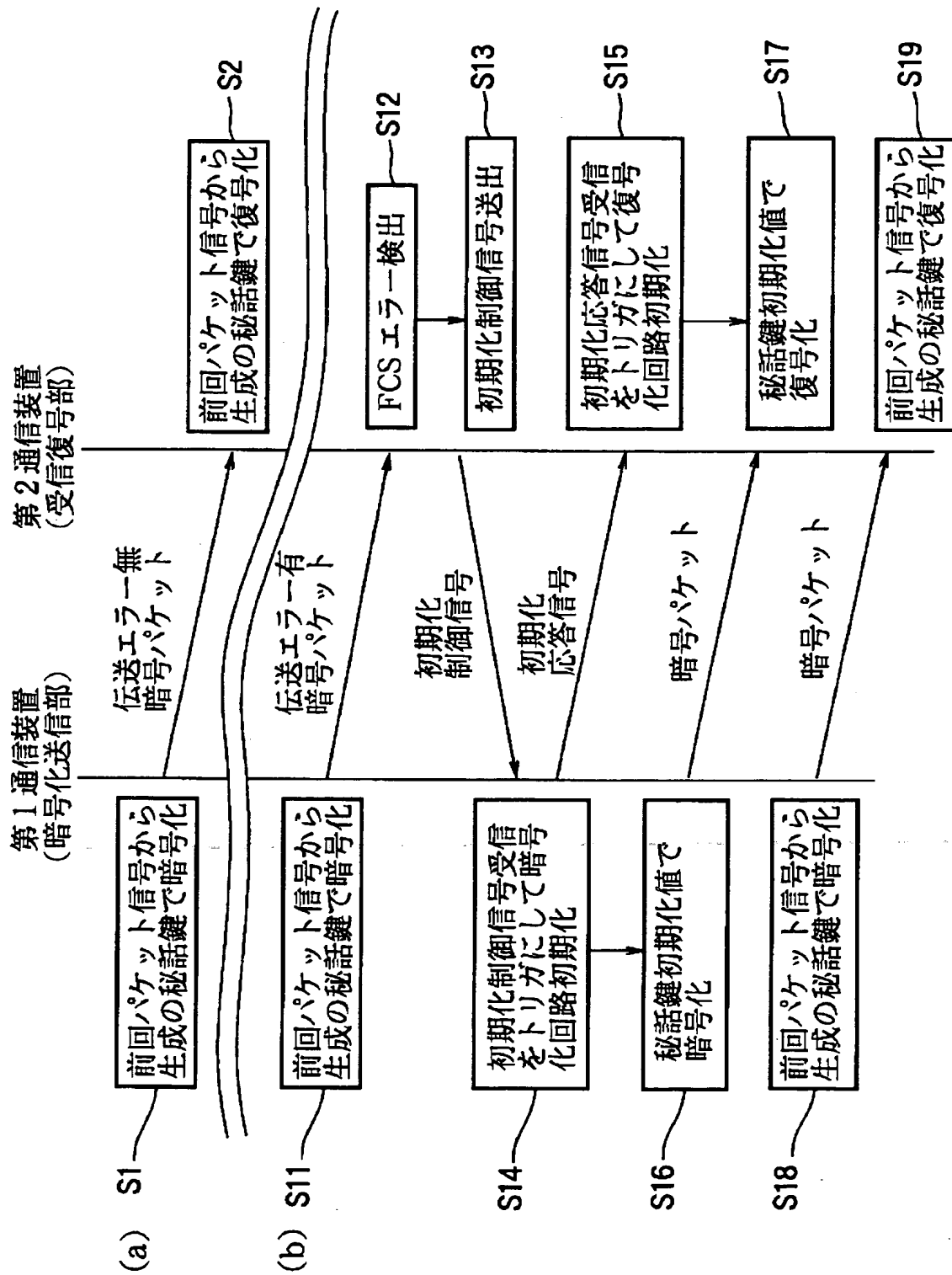
【図4】



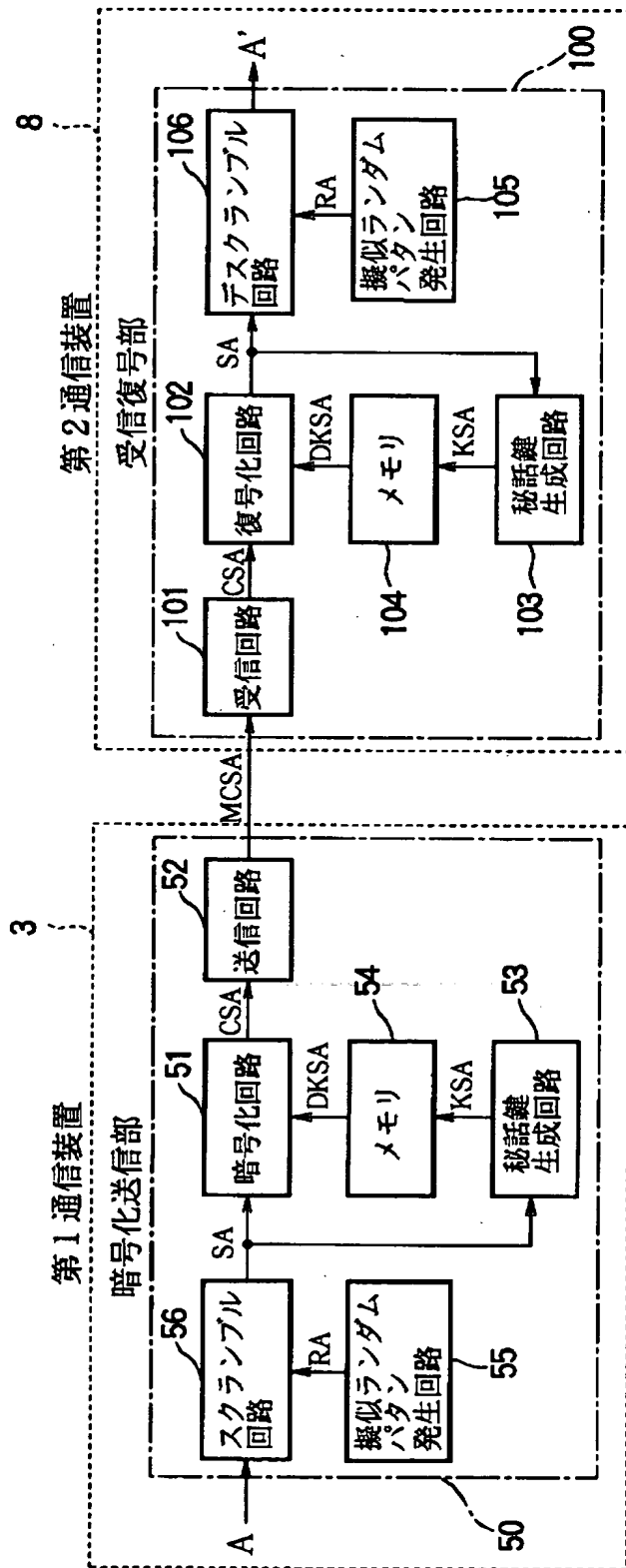
【図5】



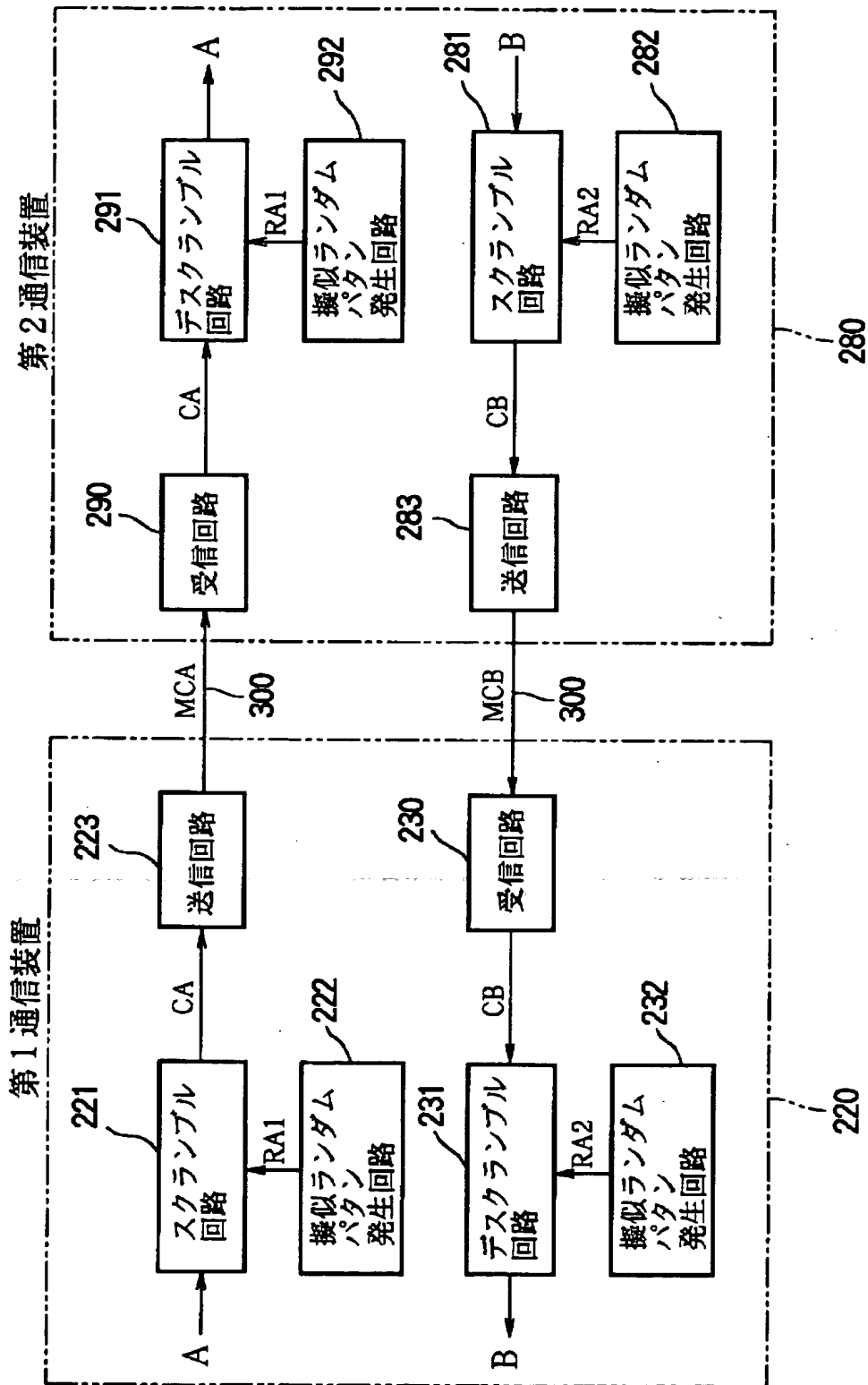
【図6】



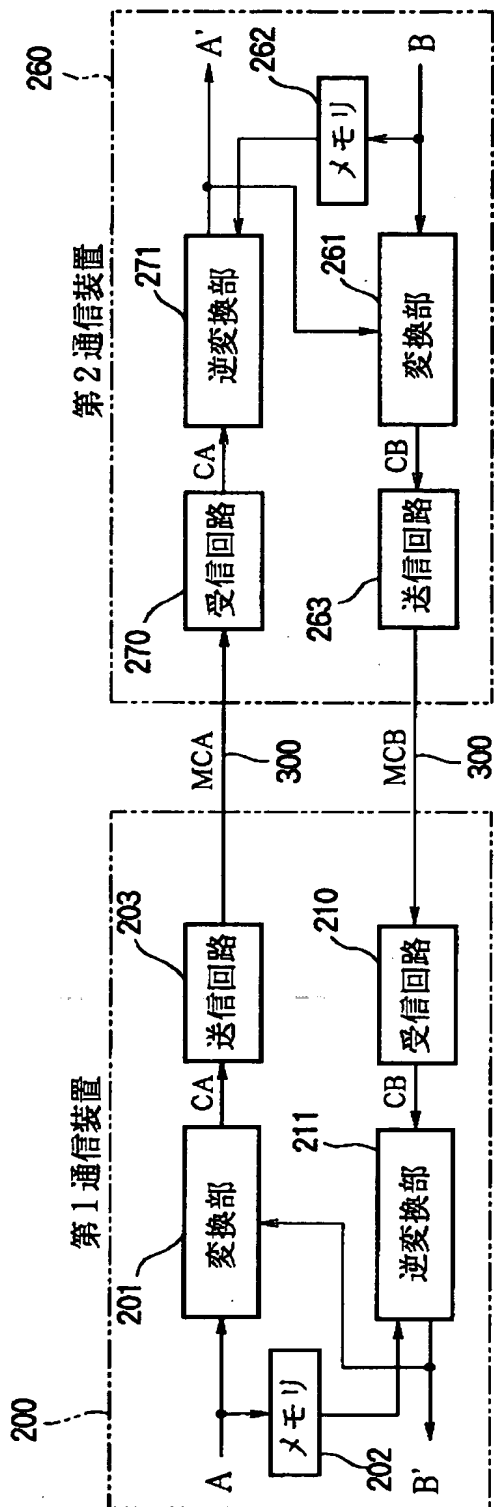
【図7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】 パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施できる簡単な構成の暗号化伝送システムを提供する。

【解決手段】 第 1 通信装置 1 は、暗号化前の第 1 の間欠信号 A に基づいて第 2 の間欠信号用の送信側秘話鍵 K A を生成する送信側秘話鍵生成回路 1 3 と、送信側秘話鍵 K A を第 2 の間欠信号の暗号化に用いるために遅延させる送信側メモリ 1 4 と、暗号化回路 1 1 とを備え、間欠信号 A に対して暗号化を実施して暗号化信号 C A（間欠信号）としてから送信回路 1 2 で送出し、第 2 通信装置 6 では、復号化後の第 1 の間欠信号 A' に基づいて第 2 の間欠信号用の受信側秘話鍵 K A を生成する受信側秘話鍵生成回路 6 3 と、受信側秘話鍵 K A を第 2 の間欠信号の暗号化に用いるために遅延させる受信側メモリ 6 4 と、受信回路 6 1 とを備えて、受信した暗号化信号 C A を復号化回路 6 2 で復号する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000000295]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	東京都港区虎ノ門1丁目7番12号
氏 名	沖電気工業株式会社